



## NYSBOE ES&S Upgrade Source Code Review Findings (Non-Central Count)

### 1.0 Introduction

Voting system certification efforts for the New York State Board of Elections by SLI Global Solutions included the verification that all of the source code modules that comprise the subject ES&S voting system were compliant with the best practices and coding requirements as described in the following documents and standards:

- VVSG 2005, (Volume I and Volume II)
- 2011NYElectionLaw.pdf
- 6210Regulations09052008.pdf
- Ciber\_COTSStandard.pdf
- NYS\_voting\_systems\_standards-4-20(6209).pdf
- havalaw.pdf
- Table of known vulnerabilities

SLI's efforts performed for the State of New York included a secure source code review to evaluate and ensure protection against all vulnerabilities identified and described within prior ITA reports, voting system tests, risk assessment final reports, and other comparable examinations.

All source code submitted for certification was reviewed by SLI personnel at the SLI Global Solutions Compliance Testing Facility. The vendor source code, build scripts, and any modified Commercial Off-the-Shelf (COTS) code were reviewed for format, structure, and functionality. All code delivered was also reviewed using both automated and manual methods for malicious code, Trojans, and viruses. The trusted build of the reviewed source code was completed by Wyle Labs at their facility in Huntsville, Alabama on July 31 and August 1, 2012, and observed for SLI and the State of New York by SLI staff.

Since the initial certification effort, ES&S has made substantial upgrades to their previously certified system. Upgrades incorporated into the current ES&S voting system include the elimination of the Election Definition Manager (EDM) application, and inclusion of EDM's previous functionality in the current version of the ElectionWare application.



The entirety of the upgraded ES&S system's source code was initially reviewed for compliance with the 2005 Voluntary Voting Systems Guidelines (VVSG) by Wyle Labs as part of their Federal review process. As directed by NYSBOE, SLI performed an additional review of a sample of the system's source code as a verification of Wyle Labs' review, and also performed a complete review of changes made to the source code for compliance with requirements of voting system source code as described in New York State regulations. In the course of performing its review, SLI also evaluated the current states of previously described and outstanding discrepancies cited against prior submissions of the source code. The evaluation of previously described non-compliant items included reviews of items that had previously been revealed through usages of security and other automated source code review tools.

## 2.0 Scope of Review and Methodology

The objective of the source code review was to analyze changes made by the vendor to the software, and to confirm the source code's compliance with the criteria set forth by the State of New York.

### List of Methodology Criteria

Review all voting system software and firmware source code for security access controls, and determine any potential vulnerabilities.

Evaluate the effectiveness of the security access controls' specific implementations within the voting system's software.

Review the voting system's software source code to determine if the system can be executed outside the intended manner and outside of normal conditions.

Where non-catastrophic failure of a device may be the result of conditions related to source code programming, exception handling routines were examined for the appropriateness of data handling logic employed.

Review voting system software source code to verify data validation routines.

Verify telecommunications capabilities, which are not allowed in NY elections systems, are not employed.

Inspect the logic related to system and user warnings, alerts, and error messages for the appropriateness of both their placements and content.

Verify the inclusion of logic related to real time audit logging as stated in the voting standards.



Any other discovered direct violations of the aforementioned standards were noted in discrepancy reports. Discrepancy reports were provided to the system vendor for their review and remediation.

### **Verification of Wyle's Work**

An effort was also undertaken to verify Wyle Labs' VVSG review of the source code. A sample of source code from each of the AutoMARK ballot marking device, and the ElectionWare election management system projects was reviewed by SLI for compliance with the requirements of the 2005 VVSG. Only non-conformities un-related to the execution of the applications were found during SLI's verification of Wyle's review. Discovered non-conformities were consistently related to the presence and content of comments as required by the VVSG. None of the non-conformities discovered by SLI during the VVSG sample verification are considered by SLI to be of concern.

## **3.0 Overview of Findings**

Items found to be non-compliant during the review were described in discrepancy reports that were then provided to the vendor for their consideration and remediation. Items described as non-compliant included:

- 1) Declared and un-used variables
- 2) Lack of logic to log certain conditions and events
- 3) Improper dispositions of system file handles
- 4) Usages of hard-coded numeric constants without explanatory comments
- 5) Ambiguous database transaction terminations

During SLI's review of the EMS ElectionWare source code it was discovered that the source code had been subject to a reformatting and re-ordering of the contents of the individual source code files. The reformatting of the source code resulted in a code set that was not directly comparable to the last previously received and reviewed version of the same application's code. After consultation with both of NYSBOE and the system vendor, ES&S, SLI was instructed by NYSBOE to provide the last previously reviewed version of the code set back to ES&S for reformatting in a way equivalent to that performed on the new and current code set. The resultant previously reviewed and now reformatted version was then used by SLI for comparison to that contained in the newest TDP. While the equivalence of the two versions of the previously reviewed code base,



pre- and post-reformatting, has been assumed, additional verification of the equivalency of the two versions is recommended for consideration by the Board of Elections.

*Note: All findings are described in the accompanying SC Review summary report.*

## 4.0 Conclusion

While several items within the source code bases were initially cited by SLI as being non-compliant with the 2005 Voluntary Voting Systems Guidelines and New York state regulations, after a succession of source code submissions and reviews, the last of which was performed on a code set received by SLI on July 27, 2012, all except three of the non-compliant items found in the EMS, DS200, and AutoMark code bases have been satisfactorily addressed by ES&S and resolved. Only three items within the ElectionWare component's source code that were cited as being non-conforming remain open. Those three items, while they remain open, are not seen by SLI as posing a significant risk to the operation of the ES&S system.

Based on the reviews performed on the last submitted ES&S source code packages, SLI recommends the following source code versions for certification as the ES&S EVS v. 5.0.0.1 voting system:

AutoMARK VAT v. 1.8.1.1a

DS200 v. 2.7.0.1i

PowerManagementMsp430 v. 1.2.6.1a

ScannerC8051 v. 2.24.0.1a

EMS, comprised of the following component versions:

CB\_Evt v. 2.1.0.1a

CB\_XML v. 2.1.0.1a

CB\_XMLConv v. 2.1.0.1a

CreateLog v. 1.5.0.1a

Electionware v. 4.1.0.1o

ElectionWarePaperBallot v. 3.1.0.1d

ERM v. 8.6.0.2c

ERMXMLConvDLL v. 3.1.0.1a

ERMXMLDATA v. 2.1.0.1a

EssEvt v. 1.5.0.1a

EssEvtA v. 1.5.0.1a

EssEvtMsg v. 1.5.0.1a

EssXml v. 4.1.0.1a



EvtSvc v. 1.5.0.1a  
EXITWIN v. 2.1.0.1a  
libCoNG v. 1.2.0.1d  
LogEvent v. 1.5.0.1a  
MYDLL v. 2.1.0.1b  
RegUtil v. 2.1.0.1a  
RmuCli v. 1.4.0.1a  
RmuDll v. 1.4.0.1a  
RmuSvc v. 1.4.0.1b  
RSACrypto v. 3.1.0.1a  
Shell v. 2.1.0.1a  
ShellSetup v. 2.1.0.1a